Échange de clef Diffie-Hellman

```
def secretKey(g,a,b,p):
   print 'Alice calcule u=', g,'^',a,'mod',p,'=', mod(g^a,p), 'et
envoie u à Bob'
   print
   print 'Bob calcule v=', g,'^',b,'mod',p,'=', mod(g^b,p), 'et
envoie v à Alice'
   print
   print 'Alors, la clef secrète est
(',mod(g^b,p),')^',a,'mod',p,'=',mod(mod(g^b,p)^a,p),'=
(',mod(g^a,p),')^',b,'mod',p
```

```
#secretKey(g,a,b,p) such that the secret numbers are g^a mod p and
g^b mod p
secretKey(2,292,426,541)
```

```
Alice calcule u= 2 ^ 292 mod 541 = 69 et envoie u à Bob

Bob calcule v= 2 ^ 426 mod 541 = 171 et envoie v à Alice

Alors, la clef secrète est ( 171 )^ 292 mod 541 = 368 =( 69 )^ 426
mod 541
```

```
```